Ethics Advisory Briefing Paper

ICT30005 Professional Issues In IT

Ethical Dilemma: Should people who commit cyberterrorism face severe legal consequences?

Name: Chin Chun Kiat

Student ID: 102765068

Due date: 3/29/2023

Submission date: 3/29/2023

Abstract

This ethical advisory briefing paper will focus on a decision regarding an ethical dilemma: Should people who commit cyberterrorism face severe legal consequences? This ethical advisory report will discuss the appropriateness of imposing severe legal consequences on individuals who commit cyberterrorism in term of ethics by research several literature reviews which mostly consist of journal articles. The report delves into the ethical dilemma by separating its sections into background and key concepts, ethical principles, and ethical recommendations. It begins by defining cyberterrorism and exploring various elements of cyberterrorism and its potential impact. Ethical dilemmas surrounding cyberterrorism are examined through the lens of four ethical principles: utilitarianism, the Golden Rule, social contract theory, and consequentialism. Each principle is applied to justify the imposition of severe legal consequences on cyberterrorists as a means of protecting society and deterring future attacks. Furthermore, this report will provide ethical recommendations that aim to be ethically appropriate and align with relevant ethical principles. As a result, this report will offer a comprehensive understanding of why individuals who commit cyberterrorism should face severe legal consequences through ethical justification.

Table of Contents

1. Background And Key Concepts

The convergence of politically motivated terrorism and cyberspace in the sabotage of information systems is a notable phenomenon worldwide. For decades, cyberterrorism has consistently grabbed global attention and remained among the foremost security concerns. As mentioned by Iqbal (2004), cyberterrorism generally refers to politically motivated cyberattacks that are unlawful and could result in violent consequences to persons or property. Cyberattacks associated with cyberterrorism are always politically motivated, as they are conducted with the intention of achieving strategic objectives that stem from political motives (Robinson et al., 2015). Many nations worldwide have taken actions to combat cyberterrorism. For example, Setiawan (2020) discusses the actions taken by the Indonesian government in combating cyberterrorism. He stated that the Indonesian government has enacted specific laws against cyberterrorism, such as legislative reforms aiming to incorporate provisions related to cybercrimes to address cyberterrorism. Additionally, he mentioned that they have established specialized agencies dedicated to combating cyberterrorism, tasked with conducting investigations and coordinating responses to cases related to cyberterrorism. The term 'Cyberterrorism' refers to the use of illegal actions to advance certain political or social goals by intimidating or coercing a government or its citizens through threats of attack on computers, networks, and the information they contain (Gordon & Ford, 2002). Furthermore, such cyberterrorism attacks could instill terror among the population through actions that could result in violent consequences on people or property. As shown in Figure 1, various elements, with fear as an outcome and political or ideological motives as part of the top three elements out of the 10 elements of cyberterrorism. This proves the importance of fear as a result and political or ideological motives in cyberterrorism likely stems from their effectiveness in achieving the objectives of the attackers because it helps the attackers achieve their goals effectively.

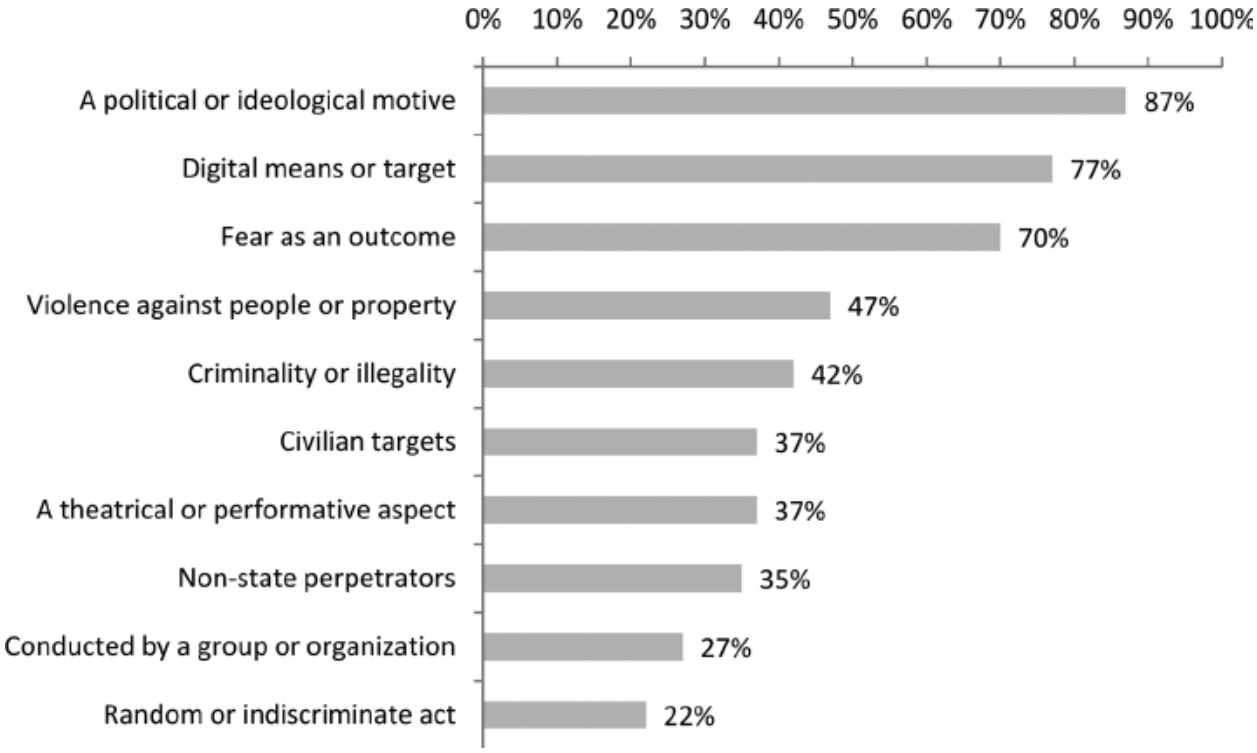

Figure 1: Various Elements of Cyberterrorism (Macdonald 2014)

There are two types of terror that could be caused by cyberterrorism, which are effect-based and intent-based (Talihärm, 2010). As stated by Talihärm (2010), the terror generated by effects-based tactics aims to instill the same level of apprehension within the population as traditional physical terrorism but through cyberspace rather than physical means. On the other hand, the purpose of intent-based terror is to coerce a government or population into adhering to specific demands or to undermine them by inflicting economic harm. Additionally, both are strategies in cyberterrorism that strive to instigate fear and wield influence, whether by instilling fear among the populace or by compelling compliance through diverse methods. Examples include attacks on critical infrastructure that may indirectly cause death or injury to the population, such as water contamination, or attacks that result in explosions or plane crashes (Dipert, 2010). There are several ways that cyberterrorism can be carried out through cyberattacks. As shown in Figure 2, different cyberattack methods such as DDOS or malware are utilized for cyberterrorism purposes, often resembling those employed in typical cyberattacks. This indicates that while cyberterrorism is politically driven, it employs the same methods as ordinary individuals who

conduct cyberattacks despite having different objectives.

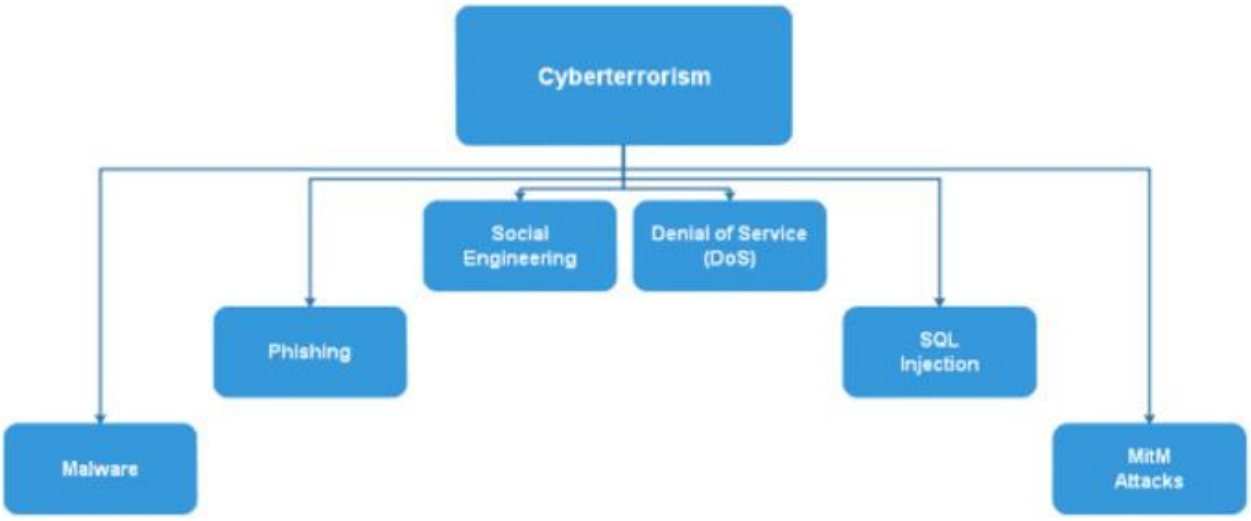

Figure 2: Methods of cyberterrorism (Iftikhar 2024)

According to World Economic Forum by Plotnek and Slay (2021), cyberterrorism such as cyber-attacks is expected to emerge as a significant global threat within the next decade. Furthermore, the potential risk of harm it causes against the humanity is significant. Herzog (2011) mentioned a notable example of cyberterrorism happened in Estonia. In 2007, Estonia's move to relocate a Soviet war memorial led to a notable cyberattack, one of the first of its scale. Perpetrators utilized a Denial of Service (DoS) attack to flood websites of government agencies, financial institutions, media outlets, and regular users. Governmental websites saw a remarkable 400-fold surge in traffic at its peak. As a result, many websites and online services had to halt their operations. The rise of cyberterrorism presents distinctive challenges for legal systems worldwide which contrast with conventional forms of terrorism. Unlike traditional acts of terrorism which manifest in the physical domain and yield direct physical consequences often resulting in physical harm, cyberterrorism operates within the cyberspace. This characteristic renders it difficult to attribute cyberattacks to specific individuals or entities. Cyberterrorism is not constrained by the physical barriers inherent in real-world scenarios, such as geographical distance (Parks & Duggan, 2005). Additionally, the internet's borderless nature further enhances cyberterrorism perpetrators to launch attacks from any place from the world, thus increase the complexities to identify and

prosecute perpetrators. Cyberterrorism has the potential to be lethal, given its connection to traditional terrorism conducted in the physical realm.

For example, Setiawan (2020) mentioned that an infamous terrorist group called 'ISIS' conducts propaganda campaigns through cyberspace to recruit members, drawing them toward Syria to bolster their ranks for further terror campaigns. Cyberterrorism can significantly impact a country's economy and political stability. Iftikhar (2024) discussed the serious impact of cyberterrorism on a nation's economy and political stability. Economically, he noted that cyberterrorism can result in direct financial losses, decreased productivity, increased security expenditures, financial theft, and damage to a nation's reputation. These attacks have the capability to disrupt business operations, forcing increased spending on cybersecurity measures. Politically, he mentioned that cyberterrorism can pose serious threats such as disrupting elections in democratic nations, spreading misinformation, invading privacy, and destabilizing governments. In the case of cyberterrorism against democratic nations, attacks on election systems erode trust in the democratic process, causing political instability, while propaganda through social media influences public opinion and may contribute more to social and political instability. Cyberterrorism represents a dual threat, impacting both the economic and political landscapes of nations.

The ethical dilemma regarding cyberterrorism is whether individuals who commit it should face severe legal consequences. One argument in favor of this stance is that cyberterrorism poses a significant threat to society, and severe legal punishments may be necessary to protect society by deterring potential future attacks. By imposing severe legal consequences on cybercriminals, it will send a powerful signal to others that such behavior will not be tolerated. This will serve as a warning to people who may consider committing cyberterrorism, which will discourage them from doing so in the future. On the other hand, critics raise concerns about the potential for disproportionate punishment, where there might be cases where individuals may have engaged in cyberterrorism unintentionally or without fully understanding the consequences of their actions.

2. Ethical Principle

There are four ethical principles that could apply to the argument supporting the stance that individuals who commit cyberterrorism should face severe legal consequences which are utilitarianism, golden rule, social contract theory and consequentialism.

2.1. Utilitarianism

Firstly, utilitarianism refers to an action being morally just if it brings more advantages than disadvantages (Sen, 1979). It suggests that the moral worth of an action is determined by its outcome or consequences. When comparing the advantages brought by the majority of the population to the minority who commit cyberterrorism, it is undeniable that the majority brings more benefits to society as a whole than the few individuals who engage in cyberterrorism, which brings more harm than benefits. However, if individuals who commit cyberterrorism do not face severe legal consequences, it could potentially put the majority of the population at risk, resulting in more harm to them. Considering the greatest good, which involves protecting most of the population from the harm of cyberterrorism, utilitarianism proves to be a suitable principle to apply in this dilemma. Regarding its application to the dilemma of individuals who commit cyberterrorism facing severe legal consequences, it is appropriate, as imposing severe legal consequences on them would deter further potential cyberterrorist attacks.

2.2. Golden Rule

Secondly, the Golden Rule is an ethical principle that refers to treating others as we would want to be treated (Weiss, 1941). It emphasizes the importance of mutual respect and understanding in fostering ethical behavior among individuals. Furthermore, one way to understand the severity of cyberterrorism and the need for consequences to deter it is to imagine the impact on the victims themselves. When individuals contemplate the impact of cyberterrorism on its victims, they can observe the significant distress it causes them. Recognizing this underscores the importance of endorsing severe legal consequences against individuals who commit cyberterrorism, aligning with the Golden Rule of treating others the way they would want to be treated. If anyone were to commit cyberterrorism and face severe legal consequences, regardless of their stance on agreeing that people who commit cyberterrorism should face severe legal consequences, they should be treated with the same legal consequences. As each of them

knows the consequences of committing cyberterrorism before they engage in such acts, especially when they stand in agreement that those who commit cyberterrorism should face legal consequences.

2.3. Social Contract Theory

Thirdly, social contract theory can also be applied to explain why individuals who commit cyberterrorism should face severe legal consequences. Social contract theory, as described by Ritchie (1891), suggests that individuals consent to be governed by society's laws in exchange for the protection of their rights and safety. It posits that people agree to relinquish certain freedoms in exchange for social order and the protection of their rights, including those who commit cyberterrorism. Individuals who engage in cyberterrorism violate this social contract by endangering the well-being of others within society through cyberspace. Therefore, severe legal consequences are justified to uphold the mutual agreement of societal order. Social contract theory emphasizes the moral obligation to safeguard the collective interests of society and the rights of everyone by deterring cyberterrorism.

2.4. Consequentialism

Finally, Sosa (1993) describes consequentialism as asserting that an action is right if its outcome is better than that of any alternative action. This means that the morality of actions is based on the positive or negative effects they produce. Consequently, we can prioritize outcomes that maximize overall benefit or minimize harm. If the use of severe legal consequences can prevent future acts of cyberterrorism, then such consequences are deemed ethically appropriate because they produce the best overall outcome compared to any alternative actions that could be taken. The principle of consequentialism justifies this approach as it prioritizes the promotion of the greater good and the prevention of potential harm.

2.5. Summary of Principles

As a result, the four ethical principles demonstrate that individuals who commit cyberterrorism should face severe legal consequences. Utilitarianism emphasizes the maximization of overall benefits for society, supporting the suggestion of imposing severe legal consequences for cyberterrorists to protect the majority from harm. Similarly, the Golden Rule underscores treating others as one would wish to be treated, supporting the notion of perpetrators facing punishment

matching the damage they caused. Social Contract Theory argues that individuals consent to societal governance in exchange for protection, justifying severe legal consequences imposed on those who commit cyberterrorism and violate this contract since they are part of society. Finally, consequentialism regards severe legal consequences as justified if they are capable of discouraging future cyberterrorism that threatens societal well-being by the outcomes of actions caused by cyberterrorists. Collectively, these ethical principles justify imposing severe legal consequences on individuals who commit cyberterrorism to safeguard society and prevent harm.

3. Ethical Recommendation

After conducting extensive research on ethical principles related to cyberterrorism, it is ethically imperative that individuals who commit cyberterrorism face severe legal consequences. Understanding the impact of cyberterrorism on others is crucial for accurately justifying the severity of legal consequences for perpetrators. There are two aspects to consider when providing recommendations: societal and governmental.

In the societal aspect, it is recommended to launch an awareness campaign to inform citizens that they should report individuals who commit cyberterrorism to the authorities. This recommendation aligns with social contract theory by Ritchie (1891), as it is the responsibility of every citizen to uphold their societal rights collectively for the protection of society. Mobilizing every citizen against cyberterrorism will protect everyone in society and is also aligned with the Golden Rule by Weiss (1941), as perpetrators of cyberterrorism should face appropriate punishment for the harm they cause to others. Additionally, individuals should understand the consequences of cyberterrorism and advocate for measures to punish those responsible.

In the governmental aspect, it is recommended that governments promote ethically appropriate punishment for individuals who commit cyberterrorism. The punishment should be severe but ethically appropriate, such as life-long imprisonment or a heavy fine. For example, in India, under section 66F of the India Code, individuals who commit cyberterrorism may face life-

long imprisonment, aligning with utilitarianism by Sen (1979) as it maximizes the benefit by preventing harm to countless individuals. Life-long imprisonment incapacitates offenders from committing further acts of cyberterrorism, sends a strong deterrent message, and protects society from harm. In the Philippines, the Cyber Terrorism Act of 2017 stipulates fines ranging from $12,000 to $600,000 depending on the severity of the cyberterrorism offense (*An Act Defining And Criminalizing Cyber Terrorism in The Philippines 2017*). Imposing heavy fines is ethically appropriate as it aligns with consequentialism by Sora (1993), focusing on maximizing overall positive outcomes. Higher fines for severe cyberterrorism offenses could deter individuals from engaging in such activities in the future, preventing harm to society, aiding in repairing affected systems, and compensating victims while reducing the resource costs for governments.

These recommendations are ethically appropriate and effective in addressing the problem of cyberterrorism, aligning with relevant ethical principles.

4. Conclusion

In summary, the definitive answer to the ethical dilemma that is key discussion of the report is to impose severe legal consequences on people who commit cyberterrorism. As outlined in this report, cyberterrorism cause threats toward individuals, governments, and economies with potential negative impacts on many different aspects. Through the research appropriate ethical principles to support the answer in chosen stance of ethical dilemma, it becomes apparent that severe legal consequences for individuals involved in cyberterrorism are justified through four ethical principles such as utilitarianism, the golden rule, social contract theory, and consequentialism due to the consequences serve as a deterrent to future potential cyberterrorism to uphold societal values and protect collective interests. Recommendations regard of decision taken in this ethical dilemma encompass societal and governmental initiatives while supported by appropriate ethical principles. By aligning actions with ethical principles and implementing proactive measures, society can mitigate the threat posed by cyberterrorism to create more secure environment for all in the most ethically appropriate way.

Reference

An Act Defining And Criminalizing Cyber Terrorism in The Philippines 2017, AmazonAWS, viewed 27 March, < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_15/HB06200.pdf>.

Dipert, RR 2010, 'The ethics of cyberwarfare', *Journal of Military Ethics,* vol.9, no.4, pp.384-410.

Gordon, S & Ford, R 2002, 'Cyberterrorism?', *Computers & Security*, vol.58, no.1, pp.636-647.

Herzog, S 2011, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security*, no.2, vol.4, pp.49-60.

Iftikhar, S 2024, 'Cyberterrorism as a global threat: a review on repercussions and countermeasures', PeerJ Comput Sci.

IndiaCode n.d., 'Section 66F: Punishment for cyber terrorism', viewed 27 March, < https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=82>.

Iqbal, M 2004, 'Defining Cyberterrorism', *Journal of Computer and Information Law*, no.2, vol.22, pp.397-408.

Macdonald, S 2014, 'What Is Cyberterrorism? Findings From a Survey of Researchers', *Terrorism and Political Violence.*

Parks, RC & Duggan, DP 2005, 'Principles of Cyberwarfare', *Security and Privacy Magazine*, vol.9, no.5, pp.30-35.

Ritchie, DG 1891, 'Contributions to the History of the Social Contract Theory', *Political Science Quarterly*, no.4, vol.6, pp.656-676.

Robinson, M & Jones, K & Janicke, H 2019, 'Cyber warfare: Issues and challenges', *Computers & Security*, vol.49, pp.70-94.

Sen, A 1979, 'Utilitarianism and Welfarism', *The Journal of Philosophy*, no. 9, vol. 76, pp. 463-489.

Setiawan, DA 2020, ‘Cyberterrorism and its Prevention in Indonesia’, *Jurnal Media Hukum*, no.2, vol.27.

Slay, J & Plotnek, JJ 2021, 'Cyber terrorism: A homogenized taxonomy and definition', *Computers & Security*, vol. 102.

Sosa, D 1993, ‘Consequences of Consequentialism’, *Mind*, no.405, vol.102, pp.101-122.

Talihärm, AM 2010, ‘Cyberterrorism: in Theory or in Practice?’, *Defence Against Terrorism Review*, no.2, vol.3, pp.59-74.

Weiss, P 1941, 'The Golden Rule', *The Journal of Philosophy*, no.16, vol.38, pp.421-430.